AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Previously Presented) A method of providing security for a computer connected to a data store via a server, the method comprising :

generating an authentication key based on a user name and a computer identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name and computer identifier; and

validating the received user name and computer identifier using the parsed user name and computer identifier,

wherein said authentication key includes a server user identifier.

2. (Original) The method of claim 1, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

3. (Original) The method of claim 2, wherein a match indicates that the received user name and computer identifier are valid.

4. (Original) The method of claim 1, further comprising, before parsing, decrypting the authentication key.

5. (Previously Presented) The method of claim 1, further comprising, if the received user name and computer identifier are valid, logging onto the server with the server user identifier and a server password.

6. (Original) The method of claim 5, further comprising, parsing the authentication key to obtain the server user identifier and server password.

7. (Original) The method of claim 6, wherein multiple users share one server user identifier and server password.

8. (Canceled).

9. (Previously Presented) The method of claim 1, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

10. (Previously Presented) The method of claim 9, further comprising encrypting the authentication key.

11. (Previously Presented) The method of claim 9, further comprising forwarding the authentication key to a user.

12. (Previously Presented) The method of claim 1, wherein the computer is connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

13. (Previously Presented) An apparatus for providing security, comprising:

a computer having a server connected thereto to access a data store;

one or more computer programs, performed by the computer, for generating an authentication key based on a user name and a computer identifier, said authentication key

includes a server user name, receiving the authentication key, the user name, and the computer

identifier, parsing the authentication key to obtain a parsed user name and computer identifier,

and validating the received user name and computer identifier using the parsed user name and

computer identifier.

14. (Original) The apparatus of claim 13, wherein validating comprises determining

whether the received user name and computer identifier match the parsed user name and

computer identifier.

15. (Original) The apparatus of claim 14, wherein a match indicates that the received

user name and computer identifier are valid.

16. (Original) The apparatus of claim 13, further comprising, before parsing, decrypting

the authentication key.

17. (Previously Presented) The apparatus of claim 13, further comprising, if the received

user name and computer identifier are valid, logging onto the server with the server user

identifier and server password.

18. (Original) The apparatus of claim 17, further comprising, parsing the authentication key to obtain the server user identifier and server password.

19. (Original) The apparatus of claim 18, wherein multiple users share one server user identifier and server password.

20. (Canceled).

21. (Previously Presented) The apparatus of claim 13, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

22. (Previously Presented) The apparatus of claim 21, further comprising encrypting the authentication key.

23. (Previously Presented) The apparatus of claim 21, further comprising forwarding the authentication key to a user.

24. (Previously Presented) The apparatus of claim 13, wherein the computer is

connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer

identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

25. (Currently Amended) An article of manufacture comprising a computer program

carrier readable by a computer connected to a server and embodying one or more instructions

executable by the computer to perform method steps for providing security to the server

connected to a data store, the method comprising:

generating an authentication key that includes a server user identifier name, based on a

user name and a computer identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name and computer identifier; and

validating the received user name and computer identifier using the parsed user name and

computer identifier.

26. (Original) The article of manufacture of claim 25, wherein validating comprises determining whether the received user name and computer identifier match the parsed user name and computer identifier.

27. (Original) The article of manufacture of claim 26, wherein a match indicates that the received user name and computer identifier are valid.

28. (Original) The article of manufacture of claim 25, further comprising, before parsing, decrypting the authentication key.

29. (Previously Presented) The article of manufacture of claim 25, further comprising, if the received user name and computer identifier are valid, logging onto the server connected to the computer with the server user identifier and server password.

30. (Original) The article of manufacture of claim 29, further comprising, parsing the authentication key to obtain the server user identifier and server password.

31. (Original) The article of manufacture of claim 30, wherein multiple users share one server user identifier and server password.

32. (Canceled).

33. (Previously Presented) The article of manufacture of claim 25, wherein the computer is connected to a client and the server and wherein the authentication key is generated with a client user name, a client computer identifier, the server user identifier, and a server password.

34. (Previously Presented) The article of manufacture of claim 33, further comprising encrypting the authentication key.

35. (Previously Presented) The article of manufacture of claim 33, further comprising forwarding the authentication key to a user.

36. (Previously Presented) The article of manufacture of claim 25, wherein the computer is connected to a client and the server, and further comprising:

at the client, transmitting the authentication key, a client user name, and a client computer identifier to the server; and

at the computer,

intercepting the authentication key; and

if the user name and computer identifier are valid, logging onto the server.

37. (Currently Amended) The method of claim 9, wherein the generated authentication

key for access to the server, is emailed to a user, and wherein when the server user identifier

changes, a new authentication key is generated and emailed to the user.

38. (Previously Presented) The method of claim 37, wherein when the client transmits

the generated authentication key, the user name and the computer identifier, to the server, the

authentication key is interecepted and validated by the computer.

39. (Previously Presented) The method of claim 38, wherein when the computer

determines that the received user name and the computer identifier match the parsed user name

and the computer identifier, the computer parses the authentication key to obtain the server user

identifier and the server password.

40. (Previously Presented) The method of claim 39, wherein the parsed server user

identifier and the parsed server password is transmitted to the server, connecting the client

computer to the server.

41. (Previously Presented) The method of claim 9, wherein the authentication key comprises the computer identifier split into portions and the portions being interposed between the user name, the server user identifier and the server password prior to encryption.

42. (Previously Presented) The method according to claim 9, wherein the computer identifier is an IP address.

43. (Previously Presented) A method of providing security for a computer connected to a data store, the method comprising:

generating an authentication key based on a user name and a computer identifier;

receiving the authentication key, the user name, and the computer identifier;

parsing the authentication key to obtain a parsed user name and computer identifier; and

validating the received user name and computer identifier using the parsed user name and computer identifier,

wherein said authentication key includes a user identifier for the computer connected to the data store.